Live Long and Migrate

Learn how Next-Generation Firewalls from Palo Alto Networks secure your migration to Amazon Web Services (AWS)

Land your migration securely

While cloud migrations have picked up steam, security risks can still threaten cloud workloads.

- Widened attack surface means more vulnerabilities
- Threats that exploit the complexity and interconnectivity of hybrid environments
- Limited visibility across sprawling data estates inhibits centralized management
- Complex compliance landscape due to the faster pace of deploying cloud workloads

The promise of increased agility, improved cost savings, and the ability to scale has propelled companies worldwide to the cloud. Today, an estimated 88 percent of businesses use cloud services in some form[1]. Many of these companies have migrated to AWS for cloud infrastructure to free up resources and lower IT costs.

Despite these ever-evolving challenges, there are plenty of organizations that have implemented successful security solutions from Palo Alto Networks to protect their environments as they migrate to AWS. Specifically, Palo Alto Networks VM-Series and CN-Series Next Generation Firewalls have delivered inline network security and threat prevention to consistently secure AWS workloads, Amazon Virtual Private Clouds (Amazon VPC), and branch locations.

While each migration to AWS is unique—with its own set of business reasons for prompting a cloud journey—VM-Series continues to be a common thread. In the following pages, you'll find migration stories of customers who have successfully moved to AWS and secured their cloud workloads with VM-Series and CN-Series.

1 O'Rielly, Cloud Adoption in 2020, May 2020

Online travel company migrates to AWS and controls outbound traffic with URL Filtering from VM-Series

COVID-19 forces reduction in operational overhead.

When COVID-19 forced many of its employees to begin working from home, a large online travel company sought to reduce its operational overhead by migrating the backend of its travel sites to AWS.

VM-Series URL Filtering secures outbound API calls.

At first, the network team tried to use an open source security product to secure API calls between the company's travel sites and external resources. But once running on AWS, the product's limitations were exposed. VM-Series virtual firewalls helped plug the gap with URL Filtering by enabling the network team to monitor and control all outbound traffic, ensuring their sites were accessing known, safe resources.

After the company implemented VM-Series in its AWS environment, it deployed the same firewall functionality in its on-premises edge environments using Palo Alto Networks hardware firewalls. In addition to URL Filtering, the information security team also replaced their discrete intrusion prevention system solution by turning on the Threat Prevention service on their Palo Alto Networks firewalls. The WildFire Malware Analysis service further augmented the setup to protect against zero-day attacks.

To simplify security management in its new hybrid cloud environment, the company relies on Panorama, which enables centralized management of all Palo Alto Networks firewalls (hardware, virtual, and containerized), as well as security services enabled on the firewalls. The company is now able to manage its public cloud and edge network security posture consistently from a single console.

Insurance company brings over on-premises policy enforcement with VM-Series during AWS migration

Modernization plan calls for leaving the datacenter business.

Like many enterprise organizations, a medium-sized insurance company sought to leave the business of running its own datacenter to reduce its technology spend and devote more time to its core product. Cost and the ability to move fast was a major driver to migrate its on-premises workloads to AWS. Licensing for the aging servers continued to increase as demand for the product fell. In addition, the company was also paying to rent physical datacenter space. As it began decommissioning its on-premises servers and migrating workloads to AWS, the company set up a hybrid architecture with an Amazon VPC to meet its low latency and local data processing needs.

VM-Series and Panorama ensure same on-premises policy model in Amazon VPC.

After many years of securing its datacenter with Palo Alto Networks hardware firewalls, the company decided to use the same security solution via VM-Series to protect its Amazon VPC. A virtual private network (VPN) tunnel was used to securely connect the on-premises datacenter to the new AWS environment. The company seamlessly enabled its on-premises policy model on its new implementation of VM-Series to ensure the same level of trusted security on AWS while it migrated workloads. Using Panorama, the company can now manage its security policies across its on-premises and AWS.

Healthcare IT company ensures application-level traffic control with VM-Series, CN-Series and consolidated workflows on AWS

Acquisition leads parent company to merge technologies in the cloud.

A small healthcare IT company that sells a Software-as-a-Service (SaaS) product was acquired, but instead of re-platforming its datacenters to merge technologies, the parent company decided to consolidate all workloads on AWS. This allowed the acquiring company to avoid the technical debt of operating another datacenter and take advantage of cost-saving options in the cloud. In addition, the company could modernize its SaaS application once on AWS.

VM-Series enables secure communications, while CN-Series brings container-level protection.

Once deployed on AWS, VM-Series firewalls were deployed in the company's application development and testing environments. VM-Series acted as an IPsec VPN termination point to enable secure communications to and from AWS. It also provided control over application-level traffic to prevent threats from moving laterally between workloads and stop data exfiltration. By integrating VM-Series with Amazon GuardDuty and AWS Security Hub, VM-Series automatically updated security policies to block malicious traffic.

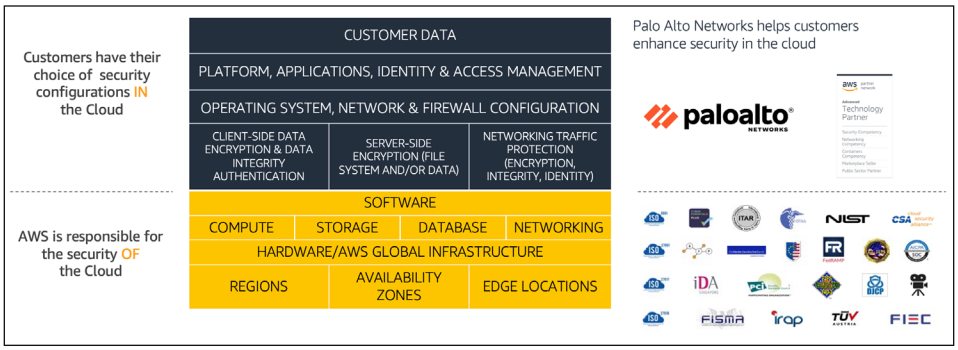
As the newly merged company began plans to rearchitect its SaaS application, it looked to containers and Kubernetes to gain efficiencies. CN-Series container firewalls delivered container network security and protected inbound, outbound, and east-west traffic that traversed Kubernetes
trust boundaries.

However you migrate, AWS and Palo Alto Networks deliver comprehensive cloud security

VM-Series and CN-series firewalls protect your AWS virtual and containerized workloads with next-generation security features that allow you to confidently and quickly migrate your business-critical applications to the cloud.

Strong security postures leverage the Shared Responsibility Model

AWS manages and controls components from the host operating system and virtualization layer, down to the physical security of the facilities in which the services operate, while AWS customers are responsible for building secure applications. Palo Alto Networks provides a wide variety of best practices documents and automation templates so you can seamlessly protect your applications on AWS from a wide range of threats.



Security services that work in concert to stop breaches

Attacks can come in multiple forms and stopping one tactic often isn't enough. Palo Alto Networks provides defense in depth with different protections throughout the attack lifecycle.

VM-Series and CN-Series

Protect networks and prevent a wide range of threats with industry-leading intelligent network security

Prisma Cloud

Secure cloud applications and maintain compliance across the entire development lifecycle

Cortex XSOAR

Unburden security teams with automated incident response and security workflows

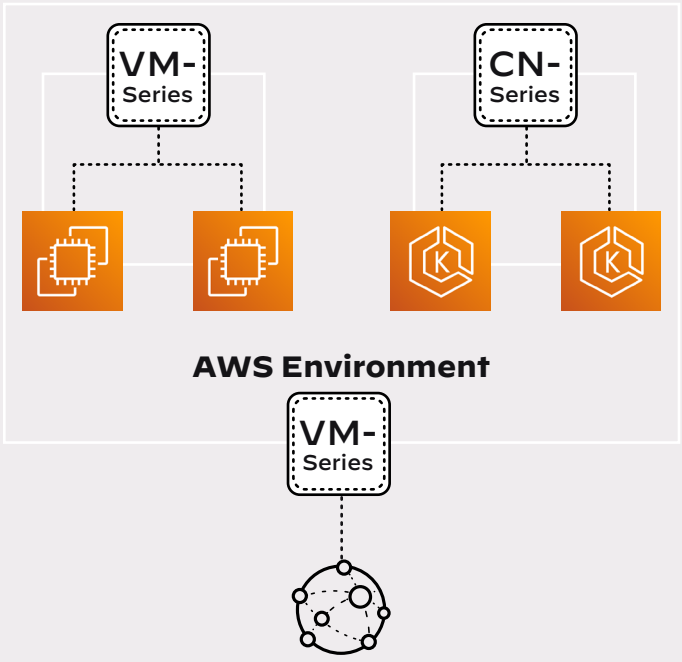
Not your average firewall

VM-Series: ML-powered, next-generation firewall

VM-Series is a new type of firewall—with machine learning (ML) and analytics at its core, capable of identifying new threats and devices without relying on fingerprinting or signatures. It continuously updates its ML models by analyzing data using unlimited cloud compute. And VM-Series reduces risk by inspecting all traffic—regardless of port or protocol—to prevent threats and mitigate exfiltration, so you can stay ahead of emerging risks and secure your entire organization.

VM-Series delivers:

- Enterprise-wide network visibility and control to protect applications and data wherever they live
- Segmentation and threat protection to minimize risk and ensure compliance
- Automated network security at scale to unshackle development teams



CN-Series: Container firewall for Kubernetes

CN-Series is one of the industry's first next-generation firewall solution built specifically to secure cloud-native applications in Kubernetes environments. CN-Series enables companies to immediately gain deep, Layer-7 visibility and control into container traffic and enforce threat prevention policies to protect allowed traffic across Kubernetes namespace boundaries.

CN-Series integrates security capabilities directly into the container environment, overcoming the visibility and control limitations of traditional firewalls deployed outside of a Kubernetes cluster. As a result, security teams have full-traffic visibility, including the ever-elusive source IP of outbound traffic, allowing them to enforce security at the application level, rather than at the cluster level.

CN-Series delivers:

- Network visibility and threat prevention in Amazon Elastic Kubernetes Service (Amazon EKS) deployments
- Frictionless deployment as part of existing DevOps workflows
- Unified security management in hybrid nfrastructures

Integration and support for AWS services

Solutions from Palo Alto Networks can help you secure your migration to AWS at every step along the way. Here's how VM-Series and CN-Series work with AWS services to enable cloud migrations and application modernization.

AWS Outposts delivers a truly consistent, hybrid experience as a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility. VM-Series integrates with AWS Outposts to protect hybrid workloads.

- Secure hybrid cloud AWS Outposts deployments with Cloud Native Security Platform and VM-Series virtual firewalls
- Protect local Amazon Elastic Cloud Compute (Amazon EC2) and Amazon VPC perimeter and inter-subnet traffic in AWS Outposts
- Ensure consistent security and policy management for AWS Outposts and on-premises networks

Amazon EKS is a fully managed Kubernetes service designed for companies to run their most sensitive, mission-critical applications through containers. CN-Series protect Kubernetes environments, including Amazon EKS.

- Gain visibility and threat protection in Amazon EKS deployments
- Align cloud-native security across the Amazon EKS environment
- Streamline security insertion in DevOps
- Unify security management in hybrid infrastructures

Migrate with intelligent security

When today's roadmap initiates your company's journey to AWS, protect your environments from the threats of tomorrow with **VM-Series** and **CN-Series** firewalls.

Visit the Palo Alto Networks page in the AWS Marketplace to learn more.

Take an Ultimate Test Drive, or see what's on your network right now through a free Security Lifecycle Review to gain unprecedented visibility into the threats and risks present in your environment.

© 2021 Palo Alto Networks, Inc. | All Rights Reserved.